Service Level Agreement

(Leistungsbeschreibung)

Inventory as a Service

Code: FS-KIE
Version: 3.0
Gültig ab 01.01.2025

CANCOM Austria AG // Wienerbergstraße 53 // 1120 Wien // Österreich // T +43 50 822 0 // info@cancom.com
HG Wien FN 178368g // Firmensitz Wien // UID ATU46276408 // InterzeroNr. 155219
Raiffeisenlandesbank Oberösterreich // BIC: RZOOAT2L // IBAN: AT35 3400 0000 0009 7899 // Creditor-ID: AT17ZZZ00000029797
www.cancom.at

Leistungen des Auftragnehmers

Dieses Dokument beschreibt die Serviceleistungen des Servicemoduls, welche im Rahmen des zwischen dem Auftraggeber (AG) und Auftragnehmer (AN) abgeschlossenen Vertrages erbracht wird. Die Verantwortlichkeiten der beschriebenen Leistungen sind auf Basis eines RACI-Modells abgebildet. Begriffserklärungen sowie Kontakt Informationen des Customer Service Center sind unter folgendem *Link* zu finden.

Sofern nichts Gegenteiliges vereinbart ist, gelten standardmäßig folgende Serviceziele: Servicezeit „SNAZ“ (NWH) mit einer Reaktionszeit von 4 Stunden.

Inventory as a Service

Mit dem Einsatz der Inventory Engine lassen sich die wichtigsten Fragen und Problemfelder rund um eine Netzwerkinfrastruktur beantworten.

Initiale Leistungen	AN	AG
Imaging der Appliance: letztstand Betriebssystem inkl. Patches, letztstand der Auftragnehmer Applikation	R/A	C/I
Vorkonfiguration der Inventory Engine (Hardware Appliance, Mini-Industrieserver) bzgl. Daten des Auftraggebers (IP Adresse, DNS/NTP etc.), danach Versand zum Auftraggeber	R/A	C/I
Remote Inbetriebnahme und Anpassung bzgl. Auftraggeber-Setup (Mailrelay, LDAP Anbindung, etc.)	R/A	C/I
Definition der zu verwaltenden Managementnetzwerke bzw. Hosts	R/A	C/I
Verbindungstests zu den Infrastruktur-Devices (Switches, Router, Accesspoints etc.)	R/A	C/I
Einrichtung User und Berechtigungsstruktur inklusive Notifications	R/A	C/I
Initiale Konfiguration des Discovery-Jobs	R/A	C/I
Verbindungstest (HTTPS) zum Rechenzentrum des Auftragnehmers in Wien für Datenanreicherung bzgl. EoX, Security Vulnerabilities, Licensing etc	R/A	C/I
Kontrolle Lokales- bzw. Remote-Backup	R/A	C/I
Herstellung und Test VPN Setup (Site2Site oder Client-VPN) für den Auftragnehmer, um das System regelmäßig zu patchen	R/A	C/I

Wiederkehrende Leistungen	AN	AG
Bereitstellung Linux-Appliance / Inventory Engine		
Der Auftragnehmer stellt dem Auftraggeber vor Ort eine gehärtete Linux-Appliance (Hardwareform: Mini-Industrieserver) zur Verfügung. Auf diesem System läuft die Inventors Engine und stellt eine moderne Benutzer- und Administrationsoberfläche mittels Webinterface (HTTPS) für den Auftraggeber zur Verfügung.	R/A	C/I

Das System wird initial im Rahmen der Installationspauschale für die Auftraggeber-Umgebung konfiguriert (IP Adresse, Subnetzmaske, Def-Gateway, DNS/NTP, Mailrelay, LDAP/MS-AD Anbindung usw.). Je nach Einstellung scannt das System einmal täglich die komplette Netzwerkinfrastruktur des Auftraggebers und erkennt somit Veränderungen, Abweichungen, die in so genannten Snapshots dokumentiert werden. Somit hat der Auftraggeber sozusagen eine tagesaktuelle „Live-CMDB“ von seiner Cisco Netzwerklandschaft.		
System Sicherheit		
Für das Service Inventory as a Service gelten höchste Security Standards. Es kommen ausschließlich verschlüsselte Protokolle (HTTPS, SSH) zum Einsatz, die Datenpartition des Linux-Systems ist native verschlüsselt (zweistufiges Verfahren), in der Datenbank werden keine unverschlüsselten Passwörter (Logindaten mit „salted Hashwerten“, Discovery-Credentials und APIs Tokens verschlüsselt) abgelegt. Die Kommunikation zum Rechenzentrum Wien des Auftragnehmers, zur Anreicherung der Daten (End-of-X, Security Vulnerabilities etc.), erfolgt über HTTP/TLS (TCP Port 443) zu einer einzigen offiziellen owned Public IP Adresse des Auftragnehmers in Wien. Es werden keine personenbezogenen Daten, keine Konfigurationen, keine Einstellungen oder Backups zum Rechenzentrum des Auftragnehmers übertragen. Per Sicherheitsdesign und Architektur gibt es KEINE Push-Funktion, der Auftragnehmer kann keine Verbindung zum System des Auftraggebers aufbauen oder initiieren. Die Inventory Engine holt sich aus dem Rechenzentrum des Auftragnehmers per HTTPS Informationen ab wie z.B. neue Security Schwachstellen oder End-of-X (Sales, Service, Software) Informationen, die publiziert wurden, und korreliert diese mit der Installed Base des Auftraggebers. Im Sinne größter Sicherheit und hundertprozentiger Transparenz kann der Auftraggeber selbst die übermittelten Datenfelder an den Auftragnehmer, in der Web-GUI, festlegen. Die Auswahl oder Abwahl der Datenfelder kann den Funktionsumfang der IE, je nach Wahl, etwas einschränken. Das Rechenzentrum Wien des Auftragnehmers ist nach international anerkannten Informationssicherheitsnorm wie ISO/IEC 27001 zertifiziert.	R/A	C/I
Behebung von Störungen		
Die vom Auftraggeber gemeldeten oder vom Auftragnehmer erkannten Störungen bzgl. der Linux-Appliance (Betriebssystem) oder Inventory Web-Applikation, werden durch den Auftragnehmer analysiert, bearbeitet und behoben. Beispiele sind: Fehler, Bug in der Weboberfläche, Systemabsturz, ungeplante Reloads, unvollständige Datensätze, Datenverlust, Probleme beim Erkennen von speziellen oder neuen Device Typen usw. Sollte eine sofortige Behebung von Fehlern und Störungen nicht möglich sein, oder es bestehen Abhängigkeiten zu Dritten (z.B. Cisco IOS Software) ist der Auftragnehmer bestrebt, mithilfe eines Workarounds die Auswirkungen der Störung zu minimieren. Die Behebung Störungen Dritter ist NICHT Bestandteil des Services und muss über andere bestehende Prozesse abgehandelt werden.	R/A	C/I

Bei Hardware-Defekt der vom Auftragnehmer bereitgestellten Linux-Appliance wird ein Ersatz (RMA-Austausch) mit einer maximalen Reaktionszeit von Next Business Week geboten. Es wird der zuletzt gesicherte Konfigurationsstand (Backup) der Auftraggeber herangezogen. Aus Datenschutzgründen und bzgl. vertraulicher Informationen bzw. Konfigurationen werden keinerlei dieser Daten zum Auftragnehmer übertragen oder gesichert. Die Verantwortung für ein „aktuelles“ Backup obliegt dem Auftraggeber selbst. In der Inventory Engine gibt es dazu manuelle (Web-GUI Download) oder professionelle Backup Varianten (automatisiertes, tägliches SFTP Backup), damit beim Auftraggeber vor Ort ein aktuelles Backup bevorratet wird. Im Fehlerfall der Hardware stellt der Auftraggeber den Technikern des Auftragnehmers ein IE-Backup für den Restore, die Systemwiederherstellung zur Verfügung. Gibt es Auftraggeberseitig kein Backup, so wird die Neuinstallation, Einrichtung bzw. Konfiguration, je nach Umfang und Bedarf, in Rechnung gestellt.		
Patches, Hotfixes und Security-Updates		
Der Auftragnehmer führt das Patch-Management für das Betriebssystem (Rocky Linux) in Abstimmung mit dem Auftraggeber halbjährlich durch, sofern kein akuter Handlungsbedarf vorliegt (z.B. schwerwiegende Sicherheitslücke mit CVSS 10), die unmittelbaren Eingriffe erfordert. Die Voraussetzung ist ein funktionierender, getesteter Remote-Zugriff (Citrix, VPN Lösung etc.) zwischen dem Auftragnehmer und dem Auftraggeber, und zumindest eine temporäre HTTPS Freischaltung ins Internet, um die Betriebssystem Pakete (RPMs) zu aktualisieren. Die eigene Web-Applikation des Auftragnehmers kann über die Weboberfläche durch den Auftraggeber selbst aktualisiert und gepatched werden. Laufend fließen Produktverbesserungen, neue Funktionen und Hotfixes ein, die der Auftraggeber selbständig mittels Bestätigung downloaden und einspielen kann. Beim Neustart der Appliance oder der Web-Applikation gibt es KEINE Beeinflussung auf Services des Auftraggebers! Das System ist ein wertvoller Helfer in der Netzwerk Infrastruktur, ist aber keinesfalls am Datentransport beteiligt. Durch ReadOnly-SSH Zugriffe (diverse Show Befehle) ist auch hundertprozentig sichergestellt, dass es in der Umgebung des Auftraggebers zu keinen Veränderungen durch unser Inventory as a Service kommt. Der Neustart oder stoppen der Dienste auf der Inventory Engine haben keinen Service Impact beim Auftraggeber!	R/A	C/I

Mitwirkungspflichten des Auftraggebers	AN	AG
Bereitstellung User und Berechtigungen		
Der Auftraggeber stellt sicher, dass es auf allen einzubindenden Geräten (Switches, Router, WLAN Controller etc.) einen Read-Only SSH-User für die Inventory Engine gibt. Die Read-Only Rechte können mittels TACACS Protokoll zusätzlich auf dedizierte „Show-Befehle“ eingeschränkt werden. Natürlich können bestehende User verwendet werden, für eine bessere Trennung und Nachvollziehbarkeit wird ein separater User für das „Inventory as a Service“ empfohlen. In großen Umgebungen kommt meist ein zentraler Verzeichnisdienst zum Einsatz (z.B. Microsoft Active Directory) der mittels RADIUS Server (z.B. Cisco ISE, MS NPS etc.) der Netzwerkinfrastruktur zur Authentifizierung zur Verfügung steht. In diesen Fällen erstellt der Auftraggeber einen zentralen Benutzer für die Inventory Engine, der auf allen Geräten funktioniert. Die Anlage des Read-Only SSH-Users ist eine wichtige Voraussetzung auftraggeberseitig. Niemals sind Write-Rechte, also Schreibbefehle oder Konfigänderungen, mittels der Inventory Engine erforderlich.	C/I	R/A

Es ist ein passives System für Lifecycle und Assetinformationen, kein Management oder Monitoring Tool etc. Der Auftraggeber sorgt für eine funktionierende Verbindung, IP-Kommunikation zwischen der Inventory Engine und den zu verwaltenden Netzwerk-Geräten (Router, Switches usw.). Sämtliche Anpassungen wie Routingtabellen, Access-Listen, Firewall-Regeln, NAT-Regeln, VPN Tunnel Erweiterungen, Provideranpassungen, WAN Anpassungen (MPLS/SD-WAN) usw., oder umfangreiche Fehlersuche, sind bzgl. dieser Punkte nicht im Dienstleistungsumfang enthalten und sind auftraggeberseitig zu bewerkstelligen.		
Voraussetzung: Secure Shell		
Geräte die per Default keine Secure Shell (SSH) bieten oder aktiviert haben, z.B. Wireless-LAN Controller, Cisco ISE usw. sind vom Auftraggeber vorzubereiten, sofern sie mittels der Inventory Engine verwaltet werden sollen.	C/I	R/A

Rahmenbedingungen für die Leistungserbringung

Bei Ende des Vertragsverhältnisses wird die Löschung der Daten des Auftraggebers durch den Auftragnehmer innerhalb eines Monats durchgeführt. Auf Wunsch können vor der Löschung die bestehenden Daten des Auftraggebers kostenpflichtig auf Medien kopiert und übergeben werden.

Nicht enthaltene Leistungen

Konfiguration des SSH-Users für die Inventory Engine auf den zu verwaltenden Geräten, oder dem zentralen Verzeichnisdienst (RADIUS)
Freischaltung oder Aktivierung von SSH auf zu verwaltenden Geräten
Konfigurationsanpassungen & intensives Troubleshooting bei Kommunikationsproblemen zwischen Inventory Engine und den Netzwerkkomponenten des Auftraggebers: Routingtabellen, Access-Listen, Firewall-Regeln, NAT-Regeln, VPN Tunnel Erweiterungen, Provideranpassungen, WAN Anpassungen (MPLS/SD-WAN) usw.
Konfigurations Änderungen auf den zu verwaltenden Geräten (Router, Switches, APs etc.)
Updates/Upgrades auf der Netzwerkinfrastruktur
Realtime Monitoring der Engine, die beim Auftraggeber steht (Auftraggeber bindet die Inventory Engine ins bestehende Monitoring-System ein)
Einrichten von neuen Funktionalitäten (Features)
Anfertigen von Spezialberichten
Cisco Geräte bzw. Produkte die nicht im LAN, WAN, WLAN, DC Bereich sind Netzwerkinfrastruktur von Dritten (z.B. Aruba, Fortinet, Avaya, Juniper usw.)
Reports mit sicherheitsrelevanten Informationen aus den Logs